(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－31958
（Ｐ2000－31958Ａ）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ	５Ｂ０４５
Ｇ０６Ｆ	13/00	３５１	Ｃ０６Ｆ	13/00	３５１Ｈ	５Ｂ０８９
	15/16	４３０		15/16	４３０Ｂ	５Ｋ０１３
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｅ	５Ｋ０６７
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ	7/26	１０９Ｒ	

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平10－202007

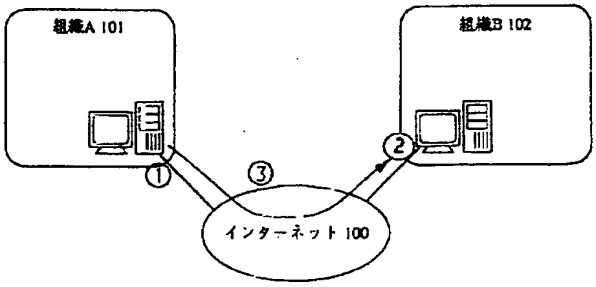
(22)出願日　平成10年７月16日(1998.7.16)

(71)出願人　000006622
株式会社安川電機
福岡県北九州市八幡西区黒崎城石２番１号
(72)発明者　中村　高幸
福岡県北九州市八幡西区黒崎城石２番１号
株式会社安川電機内
(74)代理人　100073874
弁理士　萩野　平　（外４名）

Ｆターム(参考)　5B045 BB47 GG01 JJ21 KK00
5B089 GA25 GB08 KC58
5K013 AA03 AA08 CA17 GA02 GA07
GA08 JA00
5K067 AA33 BB21 DD51 EE02 EE10
HH23 HH36

(54)【発明の名称】　移動エージェントの認証方法

(57)【要約】
【課題】　不正なエージェントからシステムを守る認証手続きを可能とする。
【解決手段】　ネットワーク100 中の複数の受信側システムを移動する移動エージェントと、該移動エージェントを生成してネットワーク中に送り出す送信側システムと、からなる移動エージェントシステムにおいて、移動エージェント３が一時的な公開鍵Kpo 、移動エージェントの送信側１が一時的な秘密鍵Kso および秘密鍵Ksを持ち、受信側２が送信側１の公開鍵Kpを持って、受信側２が移動エージェントの受信時に公開鍵Kpにより暗号化したメッセージを発し、移動エージェントにおいて一時的な公開鍵Kpo により二重に暗号化して送信側１へ送り、送信側１で秘密鍵Ksと一時的な秘密鍵Kso によりメッセージを解読して、再度一時的な秘密鍵Kso で暗号化して移動エージェントに渡し、移動エージェントは再暗号化されたメッセージを解読して受信側２へ渡し、受信側２は元のメッセージと照合する。



【特許請求の範囲】
【請求項１】　ネットワーク中の複数の受信側システムを移動する移動エージェントと、移動エージェントを生成しネットワーク中に送り出す送信側システムとからなる移動エージェントシステムにおいて、
前記移動エージェントが一時的な公開鍵、前記移動エージェントの送信側システムが一時的な秘密鍵および秘密鍵を持ち、受信側システムが前記送信側システムの公開鍵を持ち、前記受信側システムにより生成される任意のメッセージと前記一時公開／秘密鍵ペア、前記公開／秘密鍵ペアとを用いることにより前記移動エージェントの認証を行うことを特徴とする移動エージェントの認証方法。
【請求項２】　前記送信側システムの秘密鍵に対する公開鍵を前記受信側システムがあらかじめ持たずに前記移動エージェントが保持し受信側システムへ移動することを特徴とする請求項１記載の移動エージェント認証方法。
【請求項３】　前記受信側システムが、実行を許す前記移動エージェントの前記送信側システムの公開鍵の一覧を保持していることを特徴とする請求項１記載の移動エージェント認証方法。
【請求項４】　前記受信側システムは、送信側システムの秘密鍵に対する公開鍵を前記移動エージェントの移動時に外部より獲得することを特徴とする請求項２記載の移動エージェント認証方法。
【請求項５】　前記受信側システムは移動エージェント受信時に任意の認証用メッセージを生成し前記公開鍵により暗号化して移動エージェントに渡し、前記移動エージェントは前記認証用メッセージを前記一時的な公開鍵により二重に暗号化して前記送信側システムへ渡し、前記送信側システムは前記認証用メッセージを前記一時的な秘密鍵および秘密鍵により解読した後、前記認証用メッセージを前記一時的な秘密鍵により再度暗号化して前記移動エージェントへ送り、前記移動エージェントは前記認証用メッセージを前記一時的な公開鍵により解読して受信側システムへ渡し、前記受信側システムは前記認証用メッセージを保存する認証用メッセージと照合して前記移動エージェントの認証を行うことを特徴とする請求項１記載の移動エージェント認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク中の複数のシステムを移動するプログラムである移動エージェントの認証技術に関するものである。
【０００２】
【従来の技術】従来のリモートプログラミングは、例えば、図１４に示すように、第１のコンピュータシステム３００Ａ、第２のコンピュータシステム３００Ｂ、・・・等がネットワーク３５６を介して接続されているような場合に、クライアントプロセス３５２として第１のコンピュータシステム３００Ａで実行されるプロセスが、第２のコンピュータシステム３００Ｂで実行されるサーバプロセス３５４に、リモートプログラムを作成して、そのインストラクション（命令）リストを送出（３５８）し、そこで、クライアントプロセス３５２からのリモートプログラムは、サーバプロセス３５４により実行され、実行レポを受信（３６２）して終了するといった方式であったが、ネットワークにおける効率性の問題があったので、これを改善するために、特開平７－１８２１７４号には、コンピュータネットワークの「リモートプログラミングの実施方法」として、エージェントクラスおよびプレイスクラスを含む複数のオブジェクト指向クラスを定義し、オブジェクト指向クラス、オブジェクト指向クラスのサブクラス及びｇｏオペレーションを含む、コンピュータプロセスのためのインストラクション（命令）を形成する方式が提案されている。
【０００３】図１５はリモートプログラミングの実施方法の構成図であり、コンピュータシステム１２０Ａは、プレイス２２０Ａおよびエージェント１５０Ａを実行する。エージェント１５０Ａはプレイス２２０Ａを占有している。一方、コンピュータシステム１２０Ｂはプレイス２２０Ｂを実行している。（なお、エージェント又はプレイスが、特定のプレイスを占有しているということは、そのエージェント又はプレイスが、その特定のプレイスを含むコンピュータ内で実行されていることを意味している）先ず、エージェント１５０Ａがシステムにインストラクションを送出すると、ネットワーク中のプロセッサがインタープリートし、エージェント１５０Ａはこのインストラクションに応答して、例えば、プレイス２２０Ｂ（インストラクション中に特定されている）に移送される。このインストラクションは“ｇｏ”と呼ばれ、特にエージェント１５０Ａによるオペレーション“ｇｏ”の遂行と呼ばれる。エージェント１５０Ａによって、オペレーション“ｇｏ”が遂行されると、（１）、システム１２０Ａにおけるエージェント１５０Ａの実行は中止され、（２）、エージェント１５０Ａは、実行状態を保存する標準化形態に符号化されて、（３）、エージェント１５０Ａの標準化形態は、コンピュータシステム１２０Ｂへ移送され、（４）、保存された実行状態を含むエージェント１５０Ａは標準化形態からデコードされて、（５）、コンピュータシステム１２０Ｂ内において、エージェント１５０Ａの実行が再開される。こうしてエージェント１５０Ａによってオペレーション“ｇｏ”が遂行された後は、図１６に示すように、エージェント１５０Ａはもはやプレイス２２０Ａを占有していないし、コンピュータシステム１２０Ａにおいて実行されていない。その代わりにエージェント１５０Ａはプレイス２２０Ｂを占有し、コンピュータシステム１２０Ｂ内で実行されている。このように、エージェ

ントの実行の最中に遠隔のシステムにエージェントが自由に、効率的に、移動可能となる。また、ネットワーク中を自由に移動するプログラムとしての移動エージェントは、オペレーティングシステムおよびハードウェアが異なるコンピュータシステムにおいても、移動し実行可能となる。

【０００４】

【発明が解決しようとする課題】しかしながら、上記従来例においては、ネットワーク中をプログラムが移動する移動エージェントシステムの場合、受信側システムが素性を偽った不正なエージェントの要求を実行しないようにするためには、受信システムが移動エージェントの素性を知らなければならないという問題があった。そこで、本発明は、素性を偽った不正なエージェントの要求が実行されることなく、正当なエージェントの要求のみが実行可能な移動エージェントの認証方法を提供することを目的とするものである。

【０００５】

【課題を解決するための手段】上記問題を解決するために、請求項１記載の発明は、ネットワーク中の複数の受信側システムを移動する移動エージェントと、移動エージェントを生成しネットワーク中に送り出す送信側システムとからなる移動エージェントシステムにおいて、前記移動エージェントが一時的な公開鍵、前記移動エージェントの送信側システムが一時的な秘密鍵および秘密鍵を持ち、受信側システムが前記発信側システムの公開鍵を持ち、前記受信側システムにより生成される任意のメッセージと前記一時公開／秘密鍵ペア、前記公開／秘密鍵ペアとを用いることにより前記移動エージェントの認証を行うことを特徴としている。また、請求項２記載の発明は、前記送信側システムの秘密鍵に対する公開鍵を前記受信側システムが予め持たずに前記移動エージェントが保持し受信側システムへ移動することを特徴としている。そして、請求項３記載の発明は、前記受信側システムが、実行を許す前記移動エージェントの前記送信側システムの公開鍵の一覧を保持していることを特徴としている。さらに、請求項４記載の発明は、前記受信側システムが、送信側システムの秘密鍵に対する公開鍵を前記移動エージェントの移動時に外部より獲得することを特徴としている。また、請求項４記載の発明は、前記受信側システムが移動エージェント受信時に任意の認証用メッセージを生成し前記公開鍵により暗号化して移動エージェントへ渡し、前記移動エージェントは前記認証用メッセージを前記一時的な公開鍵により二重に暗号化して前記送信側システムへ渡し、前記送信側システムは前記認証用メッセージを前記一時的な秘密鍵および秘密鍵により解読した後、前記認証用メッセージを前記一時的な秘密鍵により再度暗号化して前記移動エージェントへ送り、前記移動エージェントは前記認証用メッセージを前記一時的な公開鍵により解読して前記受信側システムへ渡し、前記受信側システムは前記認証用メッセージを保存する認証用メッセージと照合して前記移動エージェントの認証を行うことを特徴としている。

【０００６】上記構成によれば、送信側システムが秘密鍵と一時的な秘密鍵を保持し、移動エージェントが一時的な公開鍵を、受信側システムが送信側システムの公開鍵を保持しているので、例えば、受信側システムは移動エージェントの認証を行う際に、移動エージェント認証用の任意なメッセージを生成し保持している公開鍵で暗号化して移動エージェントに渡し、移動エージェントは渡された認証用メッセージを一時的な公開鍵で更に二重に暗号化して送信側システムに渡し、送信側システムは渡された認証用メッセージを保持する秘密鍵と一時的な秘密鍵により解読した後、再度一時的な秘密鍵で暗号化して移動エージェントに送り、移動エージェントは一時的な公開鍵で認証用メッセージを解読して受信側システムに渡すことによって、受信側システムは受け取った認証用メッセージと保持している元のメッセージを照合すれば移動エージェントの身元を確認することができる。あるいは、送信側システムの秘密鍵に対する公開鍵は、受信側システムが予め保持していないで、移動エージェントが運び受信側システムは移動エージェントから受け取って使用することもできる。あるいは、受信側システムは公開鍵を予め持たず移動エージェント受信時に、ネットワーク内の保持しているシステムから獲得して使用することもできる。

【０００７】

【発明の実施の形態】以下、本発明の実施の形態を図を参照して説明する。図１は本発明の実施の形態に係る移動エージェント認証システムの概略構成図である。図２は図１に示す送信側システム認証部の模式図である。図３は図１に示す受信側システム認証部の模式図である。図４は図１に示す移動エージェントの認証部の模式図である。図１に示す本実施の形態の構成は、外部ネットワークとしてインターネット１００と、内部ネットワークを持つ組織Ａ１０１と、この組織Ａ１０１と関連があり内部ネットワークを持つ組織Ｂ１０２と、からなる典型的なエクストラネットを表すものであり、１は送信側システムの認証を行なう送信側認証部、２は受信側システムの認証を行なう受信側認証部、３は移動エージェントの認証を行なう移動エージェント認証部である。

【０００８】図２において、送信側システム認証部１は、一時的な公開鍵及び秘密鍵を生成する一時鍵生成手段１１、一時鍵生成手段１１により生成された一時的な秘密鍵を保持する一時鍵保持手段１２、移動エージェント３からメッセージを受信するメッセージ受信手段１３、移動エージェント３へのメッセージを送信するメッセージ送信手段１４、送信されたメッセージを解読するメッセージ解読手段１５、そのメッセージを暗号化するメッセージ暗号化手段１６、秘密鍵を保持する秘密鍵保

持手段１７、エージェントを生成するエージェント生成手段１８、生成されたエージェントを送信するエージェント送信手段１９、で構成されている。図3において、受信側システム認証部2は、移動エージェント3と会話を行うエージェント通信手段２１、移動エージェント3を介して送信側システム認証部１へ送信される任意の認証用メッセージを生成するメッセージ生成手段２２、メッセージ生成手段２２により生成された認証用メッセージを受信側システム認証部の公開鍵で暗号化するメッセージ暗号化手段２３、メッセージ生成手段２２によって生成されたメッセージを保持するメッセージ保持手段２４、メッセージ保持手段２４により保持されたメッセージと外部からのメッセージとを比較するメッセージ比較手段２５、とで構成されている。

【０００９】図4において、移動エージェントの認証部3は、一時鍵生成手段１１により生成された一時公開鍵を保持する一時鍵保持手段３１、エージェント通信手段２１とエージェント通信手段３６を介して受信側システム認証部２から送られて来る認証用メッセージを一時公開鍵により暗号化するメッセージ暗号化手段３２、送信側システム認証部より送られて来るメッセージを一時公開鍵で解読するメッセージ解読手段３３、送信側システム認証部１のメッセージ受信手段１３、メッセージ送信手段１４とやりとりを行うメッセージ送信手段３４、メッセージ受信手段３５を持ち、送信側システム認証部１が存在するシステムで生成され、ユーザの要求を書き込まれた移動エージェントの認証部である。なお、特に図示していないが、移動エージェントの操作・制御・ユーザの要求の実現を行うための手段は、送信側システム１、受信側システム２および移動エージェント3のいずれも備えているものとする。

【００１０】つぎに認証手続きを示す図５～図１３を参照して動作について説明する。図５～図１３中、１は送信側システム認証部、２は受信側システム認証部、3は移動エージェント認証部を表している。また、それぞれの丸数字は図２～図４に示す各手段の付番である。図５は図２に示す送信側システム認証部による移動エージェントの送信手続きを示す図である。図６は図3に示す受信側システム認証部のメッセージ生成手続きを示す図である、図７は図４に示す移動エージェントにおけるメッセージの二重暗号化手続きを示す図である。図８は図７に示す二重暗号化メッセージの送信側システム認証部への送信手続きを示す図である。図９は送信側システム認証部における図８に示すメッセージの解読と再暗号化手続きを示す図である。図１０は図９に示す再暗号化されたメッセージの移動エージェントへの送信手続きを示す図である。図１１は図１０に示す再暗号化メッセージの移動エージェントにおける解読手続きを示す図である。図１２は図１１に示す解読されたメッセージの受信側システム認証部への送信手続きを示す図である。図１３は解読されたメッセージの受信側システム認証部における照合手続きを示す図である。

【００１１】以下、図５～１２を用いエージェント認証手続きを順を追って説明する。先ず、図５に示すように、送信側システム認証部１で一時鍵生成手段１１により一時公開鍵Kpo と一時秘密鍵Kso が生成される。そして、エージェント生成手段１８により生成された移動エージェント3は、一時鍵保持手段３１に一時公開鍵Kpoを保存し、エージェント送信手段１９により受信側システム２へと送信される。また、一時秘密鍵Kso は、一時鍵保持手段１２により保存される。

【００１２】次に、図６に示すように、送信された移動エージェント3が受信側システム認証部２で受信されると、受信側システム認証部２のメッセージ生成手段２２により任意のメッセージM が生成され、メッセージ保持手段２４により保存されるとともに、送信側システムの秘密鍵Ksに対応する公開鍵Kpを用いて、メッセージ暗号化手段２３によって暗号化されエージェント通信手段２１に送られる。続いて、図７に示すように、暗号化されたメッセージMcはエージェント通信手段２１、移動エージェント3のエージェント通信手段３６を介して移動エージェント3に渡され、移動エージェント3内部で一時鍵保持手段３１に保存された一時公開鍵Kpo を用いてメッセージ暗号化手段３２により更に二重に暗号化され、メッセージ送信手段３４へと送られる。次に、図８に示すように、二重に暗号化されたメッセージMcc は、メッセージ送信手段３４、メッセージ受信手段１３を介して送信側システム認証部１へ渡される。続いて、図９に示すように、送信側システム認証部１に渡されたメッセージMcc はメッセージ解読手段１５において、一時鍵保持手段１２に保存されていた一時秘密鍵Kso を用いて解読され、続いて秘密鍵保持手段１７に保存されていた秘密鍵Ksにより解読される。この時点で、メッセージMcc は受信側システム認証部２のメッセージ生成手段２２で生成されたメッセージM となる。メッセージM はメッセージ暗号化手段１６において、一時鍵保持手段１２に保存されていた一時秘密鍵Kso を用いて再度暗号化されメッセージ送信手段１４へと送られる。続いて、図１０に示すように、再度暗号化されたメッセージMcは、移動エージェント3へと送られる。図１１に示すように、移動エージェント3内部でメッセージMcは、メッセージM へと解読されて、図１２に示すように受信側システム認証部２へと渡される。最後に、図１３に示すように、受信側システム認証部２へ渡されたメッセージM はメッセージ比較手段２５において、メッセージ保持手段２４に保存されていたメッセージM と比較される。比較の結果、一致すれば移動エージェント3は間違い無く送信側システム１から送られて来たものであると言える。一致しなければ、移動エージェント3は、身元不明の移動エージェントであるので受信側システム認証部２は移動エージェ

ント３を拒否し処分する。このようにして確実な認証が可能になる。なお、公開鍵Kpは受信側システムが最初から持っていても良いし、移動エージェントが来たときに、例えば認証局のような外部の機関から取って来ても良い。又は、移動エージェントが運ぶ形態でもよい。一時鍵Kpo 、Kso は移動エージェント自身や受信システムからの移動エージェントの死亡通知を受け取った時点で消去される。しかし、死亡通知を受けなくとも、あらかじめ設定された移動エージェントの寿命が尽きると共に消去される。

【００１３】

【発明の効果】以上説明したように、本発明によれば、ネットワーク中の複数の受信側システムを移動する移動エージェントと、移動エージェントを生成しネットワーク中へ送り出す送信側システムとからなる移動エージェントシステムにおいて、移動エージェントが一時的な公開鍵を、移動エージェントの送信側システムが一時的な秘密鍵および秘密鍵を持ち、受信側システムが送信側システムの公開鍵を持ち、受信側システムにより生成される任意のメッセージと一時公開／秘密鍵ペア、公開／秘密鍵ペアを用いた、送信側、受信側システムと移動エージェント間のメッセージ通信により、移動エージェントの認証を行うように構成したので、迅速正確に移動エージェントの認証ができるという効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る移動エージェント認証システムの概略構成図である。

【図２】図１に示す送信側システム認証部の模式図である。

【図３】図１に示す受信側システム認証部の模式図である。

【図４】図１に示す移動エージェントの認証部の模式図である。

【図５】図２に示す送信側システム認証部による移動エージェントの送信手続きを示す図である。

【図６】図３に示す受信側システム認証部のメッセージ生成手続きを示す図である。

【図７】図４に示す移動エージェントにおけるメッセージの二重暗号化手続きを示す図である。

【図８】図７に示す二重暗号化メッセージの送信側システムへの送信手続きを示す図である。

【図９】図８に示す二重化暗号メッセージの送信側システムにおける解読と再暗号化手続きを示す図である。

【図１０】図９に示す再暗号化メッセージの移動エージェントへの送信手続きを示す図である。

【図１１】図１０に示す再暗号化メッセージの移動エージェントにおける解読手続きを示す図である。

【図１２】図１１に示す解読メッセージの受信側システム認証部への送信手続きを示す図である。

【図１３】図１２に示す解読メッセージの照合手続きを示す図である。

【図１４】従来のリモートプログラミングの説明図である。

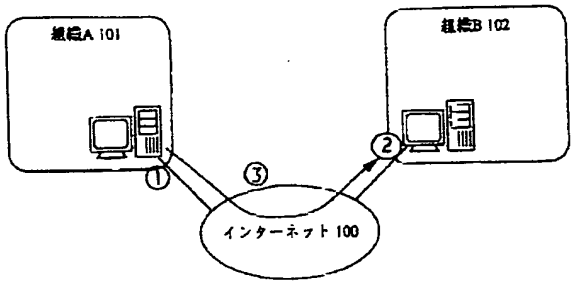
【図１５】従来のリモートプログラミングの実施方法の構成図である。

【図１６】図１５に示す移動エージェントの説明図である。

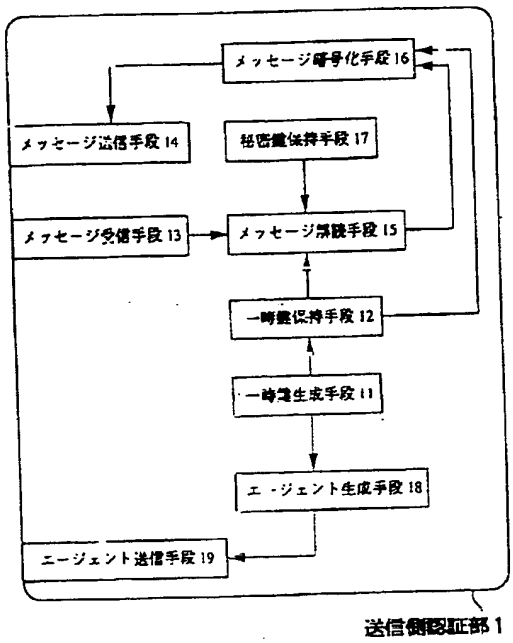
【符号の説明】

１　送信側システム認証部
２　受信側システム認証部
３　移動エージェントの認証部
１１　一時鍵生成手段
１２　一時鍵保持手段
１３　メッセージ受信手段
１４　メッセージ送信手段
１５　メッセージ解読手段
１６　メッセージ暗号化手段
１７　秘密鍵保持手段
１８　エージェント生成手段
１９　エージェント送信手段
２１　エージェント通信手段
２２　メッセージ生成手段
２３　メッセージ暗号化手段
２４　メッセージ保持手段
２５　メッセージ比較手段
３１　一時鍵保持手段
３２　メッセージ暗号化手段
３３　メッセージ解読手段
３４　メッセージ送信手段
３５　メッセージ受信手段
３６　エージェント通信手段
１００　インターネット
１０１　組織Ａ
１０２　組織Ｂ

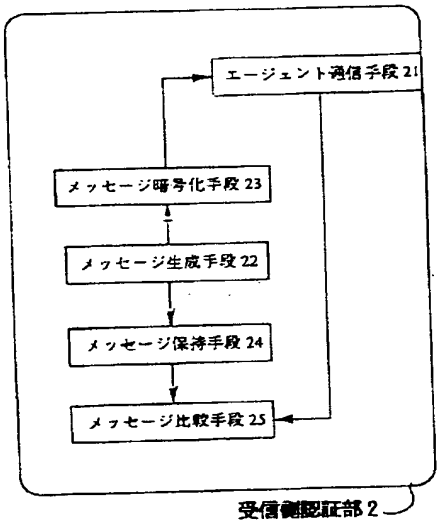
【図1】



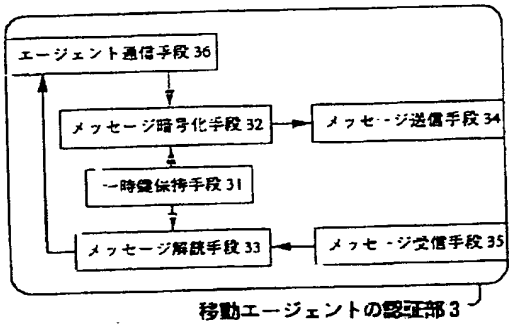
【図2】



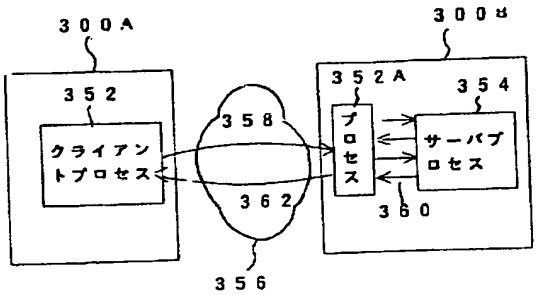
【図3】



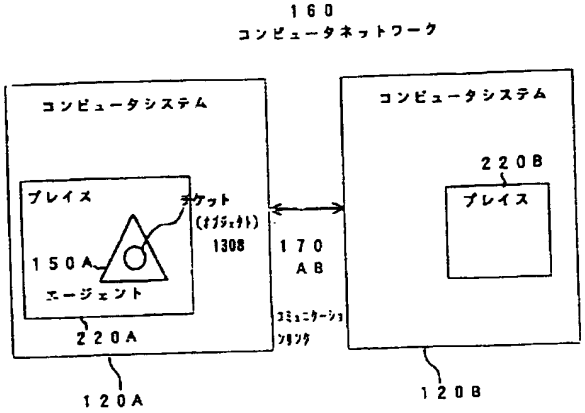
【図4】



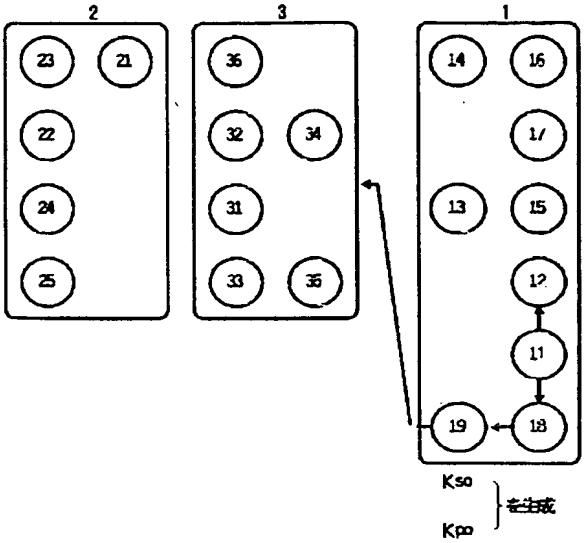
【図14】



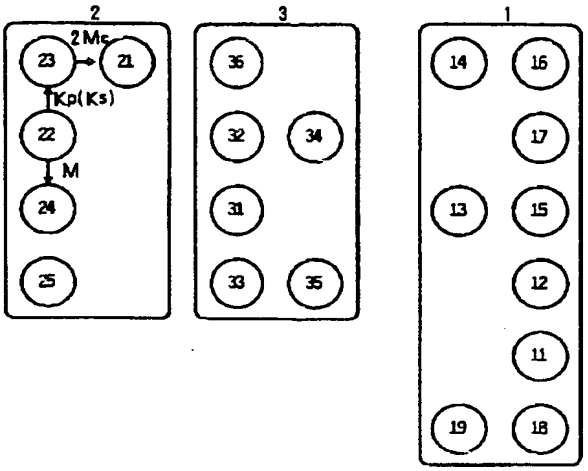
【図15】



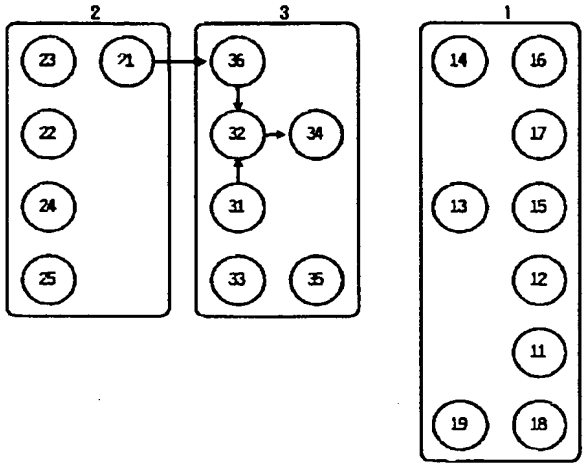
【図5】


2
3
1
23
21
22
24
25
35
32
34
31
33
36
14
16
17
13
15
12
11
19
18
Kso
Kpo
を生成

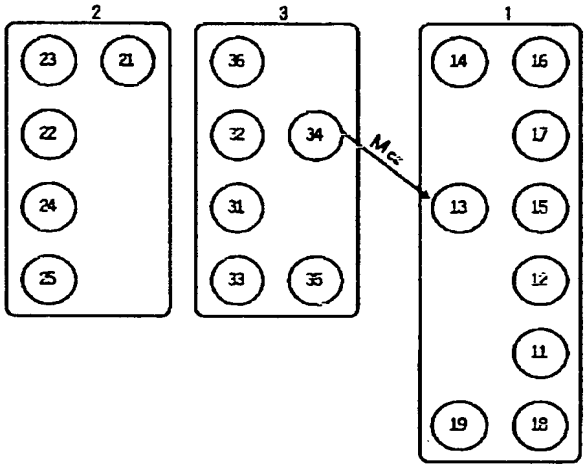
【図6】


2
3
1
2Mc
Kp(Ks)
M
23
21
22
24
25
35
32
34
31
33
36
14
16
17
13
15
12
11
19
18

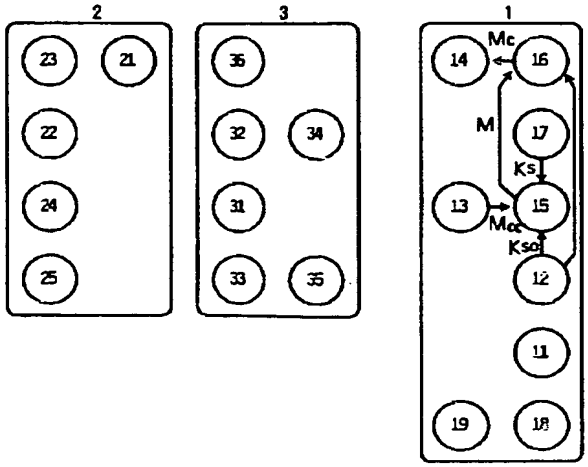
【図7】


2
3
1
23
21
22
24
25
35
32
34
31
33
36
14
16
17
13
15
12
11
19
18

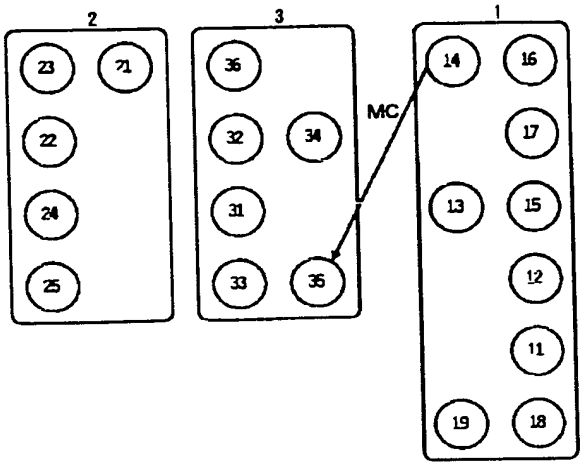
【図8】


2
3
1
23
21
22
24
25
35
32
34
31
33
36
Mc
14
16
17
13
15
12
11
19
18

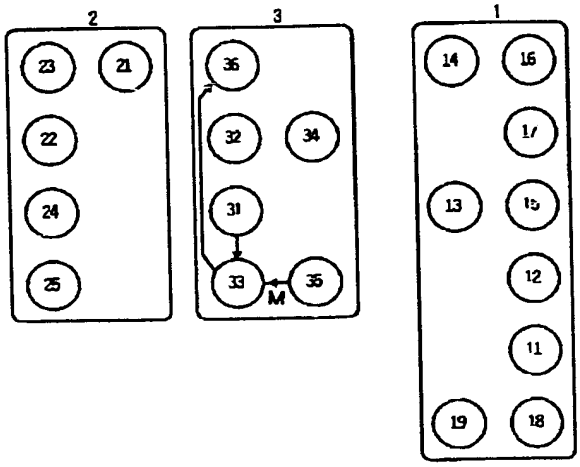
【図9】


2
3
1
23
21
22
24
25
35
32
34
31
33
36
Mc
M
Ks
Mc
Kso
14
16
17
13
15
12
11
19
18

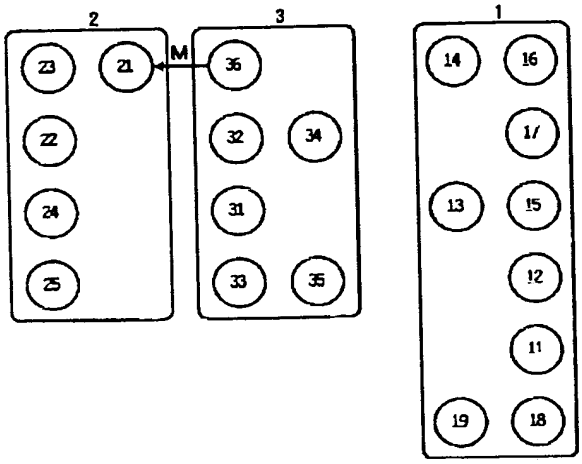
【図10】



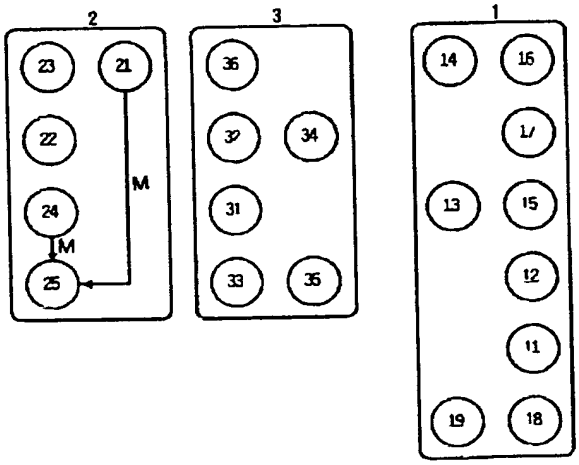
【図11】



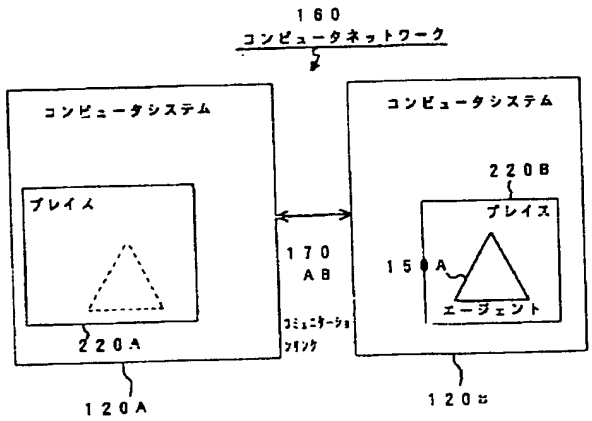
【図12】



【図13】



【図16】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
H04L 9/08		H04L 9/00	601C	
9/14			601F	
			641	